PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-098133
(43)Date of publication of application : 09.04.1999

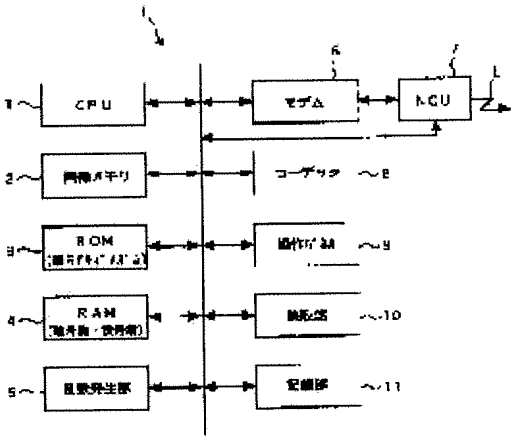
(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 9/00
H04N 1/44

(21)Application number : 09-255100
(22)Date of filing : 19.09.1997

(71)Applicant : MURATA MACH LTD
(72)Inventor : HATASHITA MASAHIRO

(54) COMMUNICATION TERMINAL EQUIPMENT AND METHOD FOR CIPHER COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To enable simple change of set data and execute secret key mode cipher communication by providing a facsimile equipment with a means for deciphering a 2nd secret key with a 1st secret key and a public key and a means for ciphering data with the deciphered 2nd secret key and transmitting the result.
SOLUTION: The facsimile equipment F is provided with a means for generating a secret key and a public key, a means for transmitting the generated public key, a means for receiving ciphered data by the transmitted public key, and a means for deciphering the ciphered data by the secret key. These means are constituted when CPU 1 executes public key mode cipher algorithm stored in a ROM 3. Namely the CPU 1 generates the 1st secret key and the public key and transmits the generated disclosed key. Then the CPU 1 controls processing for receiving the 2nd secret key ciphered by the public key and deciphering the 2nd secret key by the 1st secret key. In addition, the CPU 1 ciphers data by the deciphered 2nd secret key and transmits the ciphered data.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－98133

(43)公開日　平成11年(1999)４月９日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｇ
Ｈ０４Ｌ	9/00		Ｈ０４Ｎ	1/44	
Ｈ０４Ｎ	1/44		Ｈ０４Ｌ	9/00	
					６０１Ｅ

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平9－255100

(22)出願日　平成９年(1997)９月19日

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地

(72)発明者　畑下　真広
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内

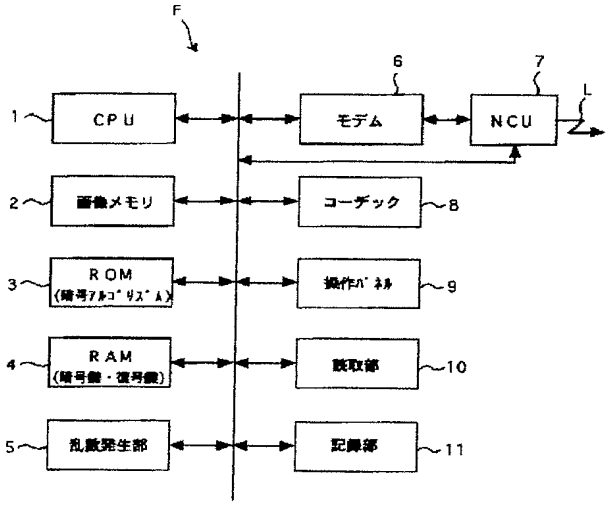
(74)代理人　弁理士　中井　宏行

(54)【発明の名称】　通信端末装置及び暗号通信方法

(57)【要約】

【課題】　簡易に設定データを変更できるようにして、秘密鍵方式の暗号通信ができるようにする。

【解決手段】　乱数発生手段５と、この乱数発生手段５が発生させた乱数に基づいて第１秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第２秘密鍵を受信する手段と、この暗号化された第２秘密鍵を第１秘密鍵と公開鍵により復号化する手段と、この復号化した第２秘密鍵によりデータを暗号化して送信する手段とを備える。



1

【特許請求の範囲】

【請求項１】乱数発生手段と、この乱数発生手段が発生させた乱数に基づいて第１秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第２秘密鍵を受信する手段と、この暗号化された第２秘密鍵を上記第１秘密鍵と公開鍵により復号化する手段と、この復号化した第２秘密鍵によりデータを暗号化して送信する手段とを備えた通信端末装置。

【請求項２】予め第２秘密鍵を設定する手段と、上記公開鍵を受信する手段と、この受信した公開鍵により上記第２秘密鍵を暗号化して送信する手段と、この暗号化した第２秘密鍵が復号化され、この復号化された第２秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを上記第２秘密鍵により復号化する手段とを、更に備えた請求項１に記載の通信端末装置。

【請求項３】送信側は、乱数に基づいて第１秘密鍵と公開鍵とを生成し、送信した公開鍵により暗号化された第２秘密鍵を受信すると、復号化した第２秘密鍵によりデータを暗号化して送信する一方、受信側は、上記公開鍵により暗号化して送信した第２秘密鍵に基づいて暗号化されたデータを受信すると、このデータを第２秘密鍵により復号化することを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ファクシミリ装置などの通信端末装置及びこの装置で使用される暗号通信方法に関する。

【０００２】

【従来の技術】従来から、ファクシミリ装置などの通信端末装置では、情報セキュリティ対策の一環として暗号通信が行われている。この暗号通信の方法は、暗号アルゴリズムを公開し、多数の者が利用できるようにしているものが主流であり、このアルゴリズム公開型暗号方式には、暗号鍵と復号鍵を同じにしてその両方を秘密にする秘密鍵方式と、暗号鍵と復号鍵を異なるものにして、暗号鍵は公開し復号鍵は秘密にする公開鍵方式とがある。

【０００３】秘密鍵方式にはＤＥＳやＦＥＡＬなどの暗号方式があり、公開鍵方式にはＲＳＡなどの暗号方式がよく用いられている。なお、秘密鍵方式は、公開鍵方式に比べて処理速度が速いという特長があるため、データ量が多い場合には特に有効に利用されている。具体的には、秘密鍵方式の場合、データの送信側と受信側の各々に、予め同じ鍵を設定しておく単純な方法以外に、一方（受信側）だけに秘密鍵を設定すればよいために、前もって、公開鍵方式を用いて、送信側から公開鍵を送信し、これによって受信側が秘密鍵自身を暗号化して送信側に返信する方法がある。送信側では、返信された秘密鍵を復号できるので、以降、これを用いて暗号化したデータを送信する。

2

【０００４】なお、この方法においても、送信側が公開鍵を所定のデータの中から任意に設定して送信し、これを基にして受信側が秘密鍵を暗号化する方法と、さらに受信側が秘密鍵を任意に設定しておき、送信側から公開鍵を受信すると、これを基に秘密鍵を暗号化する方法とに分類される。

【０００５】

【発明が解決しようとする課題】ところが、上記従来の通信端末装置では、秘密鍵方式の暗号通信において、受信側のみに予め秘密鍵を設定しておく場合でも、その秘密鍵自身の暗号通信の安全性を保つためには、送信側あるいは受信側の設定データを、定期的にキー操作などで設定しなおす必要があり、面倒であった。

【０００６】本発明はこのような事情に鑑みて提案されたものであり、簡易に設定データを変更できるようにして、秘密鍵方式の暗号通信ができるようにした通信端末装置及びその暗号通信方法を提供することを目的としている。

【０００７】

【課題を解決するための手段】上記目的を達成するために提案される請求項１に記載の通信端末装置は、乱数発生手段と、この乱数発生手段が発生させた乱数に基づいて第１秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化された第２秘密鍵を受信する手段と、この暗号化された第２秘密鍵を第１秘密鍵と公開鍵により復号化する手段と、この復号化した第２秘密鍵によりデータを暗号化して送信する手段とを備える。

【０００８】請求項１では、データの送信側となる通信端末装置について提案しており、乱数に基づいて、第１秘密鍵と公開鍵を生成するところに特徴がある。この公開鍵は、受信側の第２秘密鍵自身を暗号化させるためのものであり、公開鍵を生成したときは、同時に第１秘密鍵も生成されているので、暗号化された第２秘密鍵を受信すると、これを復号化できる。これによって、第２秘密鍵を以降のデータ送信時の暗号化に用いることができる。

【０００９】請求項２では、請求項１の構成に加えて、更に、予め第２秘密鍵を設定する手段と、公開鍵を受信する手段と、この受信した公開鍵により第２秘密鍵を暗号化して送信する手段と、この暗号化した第２秘密鍵が復号化され、この復号化された第２秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを第２秘密鍵により復号化する手段とを備える。

【００１０】すなわち、請求項２では、データの受信側となる場合を含めた通信端末装置について提案しており、公開鍵を受信すると、これを用いて第２秘密鍵を暗号化し送信する。すると、第２秘密鍵で暗号化されたデータを受信するので、このデータを第２秘密鍵により復

号化すればよい。請求項３では、請求項１及び請求項２に記載の通信端末装置が使用する暗号通信方法について提案しており、送信側は、乱数に基づいて第１秘密鍵と公開鍵とを生成し、送信した公開鍵により暗号化された第２秘密鍵を受信すると、復号化した第２秘密鍵によりデータを暗号化して送信する一方、受信側は、公開鍵により暗号化して送信した第２秘密鍵に基づいて暗号化されたデータを受信すると、このデータを第２秘密鍵により復号化することを特徴とする。

【００１１】

【発明の実施の形態】以下に、図面を参照して本発明の実施の形態を説明する。図１は、本発明の通信端末装置の構成の一例を示すブロック図である。ここでは、通信端末装置の例としてファクシミリ装置Ｆの構成例を示すが、本発明はこれに限定されることはなく、データの暗号通信機能を備えたパーソナルコンピュータ等であってもよい。

【００１２】ＣＰＵ１はこのファクシミリ装置Ｆの各部を制御する。画像メモリ２はＤＲＡＭ等で構成され、送受するファクシミリ通信データを一時記憶する。ＲＯＭ３は、公開鍵方式のＤＥＳやＦＥＡＬなどや、秘密鍵方式のＲＳＡなどの公開されている暗号アルゴリズムを記憶する他、このファクシミリ装置Ｆの動作に必要な制御プログラムなどを記憶する。ＲＡＭ４は処理の実行時に発生する一時的なデータを記憶する。乱数発生部５は、本発明の乱数発生手段を構成し、これによって発生した乱数に基づいて、公開鍵方式の暗号通信を行うべく、秘密鍵（第１秘密鍵）と公開鍵とを生成する（後述）。

【００１３】モデム６はファクシミリ通信のために信号の変調、復調を行う。ＮＣＵ７は通信回線Ｌ１（アナログ回線）の閉結、開放を行う。なお、デジタル回線を接続する場合は、モデム６及びＮＣＵ７の代わりに、ＤＳＵに接続するためのＩＳＤＮインターフェースなどを備える。コーデック８はMHやMR符号などのファクシミリ通信データに符号化又は復号化する。

【００１４】操作パネル９は、このファクシミリ装置Ｆの動作状態などを表示する液晶表示装置などの表示手段と、このファクシミリ装置Ｆに対し各種入力設定を各種キーなどの操作手段とで構成される。読取部１０は、原稿から画像を読み取りイメージデータにする。記録部１１はプリンタで構成され、他のファクシミリ装置などから受信したデータなどをイメージデータにして記録（印字出力）する。

【００１５】このファクシミリ装置Ｆは、更に、公開鍵方式の暗号通信を実行すべく、秘密鍵と公開鍵とを生成する手段と、この生成した公開鍵を送信する手段と、この送信した公開鍵により暗号化されたデータを受信する手段と、この暗号化されたデータを秘密鍵により復号化する手段とを備えている、本発明では、この暗号化されるデータが、以降に説明する秘密鍵方式の暗号通信を実現するための秘密鍵自身になっているため、このデータとなる秘密鍵を第２秘密鍵と呼び、上記公開鍵方式の秘密鍵を第１秘密鍵と呼ぶことにする。

【００１６】なお、上記した各手段は、ＲＯＭ３に記憶された公開鍵方式の暗号アルゴリズムを、ＣＰＵ１が実行することによって構成されている。つまり、ＣＰＵ１は、第１秘密鍵と公開鍵とを生成し、この生成した公開鍵を送信し、この送信した公開鍵により暗号化された第２秘密鍵を受信し、この暗号化された第２秘密鍵を第１秘密鍵により復号化する処理を制御する。

【００１７】また、このファクシミリ装置Ｆは、上述したように、秘密鍵方式の暗号通信を実行すべく、復号化した第２秘密鍵によりファクシミリデータを暗号化して送信する手段を備える。この手段は、ＲＯＭ３に記憶された秘密鍵方式の暗号アルゴリズムを、ＣＰＵ１が実行することによって構成される。なお、このファクシミリデータを送信するときの暗号方式には、上記第２暗号鍵の暗号方式と同じあるいは異なる公開鍵方式を用いることもできるが、データ量が多くなるにつれて、処理速度が遅くなることを防ぐため、秘密鍵方式を用いることが好ましい。

【００１８】本発明では、乱数発生部５が発生させた乱数に基づいて、第１秘密鍵と公開鍵を生成するところに特徴がある。これによって、いちいち操作パネル９を操作して、これらの鍵のデータを設定する必要がなくなる。以上には、このファクシミリ装置Ｆが暗号通信の送信側になる場合について説明したが、受信側になる場合は、更に、予め第２秘密鍵を設定する手段としてＲＡＭ４を備え、公開鍵方式の暗号通信を実行すべく、公開鍵を受信する手段と、この受信した公開鍵により第２秘密鍵を暗号化して送信する手段とを備える。

【００１９】これら通信の手段は、上記送信側となる場合と同様に、ＲＯＭ３に記憶された公開鍵方式の暗号アルゴリズムを、ＣＰＵ１が実行することによって構成される。つまり、ＣＰＵ１は、公開鍵を受信し、この受信した公開鍵により暗号化した第２秘密鍵を送信する処理を制御する。また、このファクシミリ装置Ｆは、秘密鍵方式の暗号通信を実行すべく、暗号化した第２秘密鍵が復号化され、この復号化された第２秘密鍵により暗号化されたデータを受信する手段と、この受信したデータを第２秘密鍵により復号化する手段とを備える。これらの手段は、ＲＯＭ３に記憶された秘密鍵方式の暗号アルゴリズムを、ＣＰＵ１が実行することによって構成される。つまり、ＣＰＵ１は、第２秘密鍵により暗号化されたデータを受信し、この受信したデータを第２秘密鍵により復号化する処理を制御する。

【００２０】図２には、上記した暗号通信方法を具体的に示している。ここでは、公開鍵方式としてＲＳＡ暗号方式を使用する場合を示している。ＲＳＡ暗号方式を説明すると、まず、十分大きな２つの素数ｐとｑを定め、

5

【数１】

$$n=pq$$

とする。

【００２１】次いで、（ｐ－１）（ｑ－１）と互いに素な正数ｅを定める。すなわち、

【数２】

$$(e,(p-1)(q-1))=1$$

である。本発明では、ｐ，ｑ，ｅといった素数が、乱数によって定められることになる。

【００２２】そして、（ｐ－１）（ｑ－１）を法とするときのｅの逆数ｄ、すなわち、

【数３】

$$ed\equiv 1(\mathrm{mod}\ (p-1)(q-1))$$

を満たすｄを求めておく。

【００２３】そして、公開鍵をｎとｅ、秘密鍵（本発明の第１秘密鍵）をｐとｑとｄとし、平文Ｍに対し、

【数４】

$$C\equiv M^{e}\ \mathrm{mod}\ n$$

として暗号文Ｃを生成する。

【００２４】これを、復号化するときには、

【数５】

$$M\equiv C^{d}\ \mathrm{mod}\ n$$

を用いて平文Ｍを求めればよい。

【００２５】例えば、公開鍵をｎ＝５５，ｅ＝７とし、秘密鍵をｐ＝５，ｑ＝１１，ｄ＝２３（$7\times 23\ \mathrm{mod}\ 40=1$）、平文をＭ＝３とすれば、暗号文はＣ＝４２（$3^{7}\ \mathrm{mod}\ 55=42$）となり、また、$42^{23}\ \mathrm{mod}\ 55=3$（＝Ｍ）によって復号できることになる。

【００２６】送信側では、乱数に基づき、数式１～３を用いて、第１秘密鍵ｐ，ｑ，ｄと公開鍵ｅ，ｎとを生成し（①）、公開鍵ｅ，ｎを送信する。これに対し、受信側は、数式４を用いて、公開鍵ｅ，ｎにより第２秘密鍵Ｋ（数式４，５では平文Ｍに相当）を暗号化して秘密鍵Ｃとして（②）、送信する。送信側は、暗号化された第２秘密鍵Ｃを受信すると、数式５を用いて第１秘密鍵ｄと公開鍵ｎにより復号化し（③）、この復号化した第２秘密鍵Ｋによりデータを暗号化して送信して（④）、これを受信側は第２秘密鍵Ｋにより復号化する（⑤）。

【００２７】次に、このときのファクシミリ装置Ｆの動作を図３と図４にフローチャートで示す。図３はデータ送信時の動作を示している。ＣＰＵ１は、操作パネル９によって送信操作がなされると、乱数発生部５で発生させた乱数を基に第１秘密鍵と公開鍵を生成し、これらをＲＡＭ４に記憶しておく。そして、公開鍵を送信した後に受信したデータ（暗号化された第２秘密鍵）を、ＲＡＭ４に記憶しておいた鍵で復号化する。その後は、読取部１０で読み取り、コーデック８で符号化して、一旦画像メモリ２に蓄積したファクシミリデータ（符号化データ）を、順次、復号化したデータ（第２暗号鍵）を用いて暗号化し、モデム６とＮＣＵ７を介して回線Ｌに対して送信する（以上、１００～１０５）。

6

【００２８】一方、図４はデータ受信時の動作を示している。ＣＰＵ１は、公開鍵を受信すると、予めＲＡＭ４に記憶している第２秘密鍵を暗号化して送信する。すると、暗号化されたファクシミリデータ（符号化データ）が、回線Ｌを通じて送信されて来るので、順次、画像メモリ２に蓄積し、ＲＡＭ４に記憶している第２秘密鍵を用いて復号化しながら、コーデック８で復号化し、記録部１１によって印字出力する（以上、２００～２０４）。

【００２９】なお、以上には、送信側で第１秘密鍵と公開鍵とを乱数に基づいて生成する場合を説明したが、さらに受信側で第２秘密鍵を乱数に基づいて生成するようにしてもよい。また、第２暗号鍵の暗号化及び復号化と、ファクシミリデータの暗号化及び復号化とは、同一の演算手段であるＣＰＵ１で行うことには限定されず、それぞれ別々の回路を用いて行うようにしてもよい。

【００３０】

【発明の効果】以上の説明からも理解できるように、本発明の請求項１に記載の通信端末装置は、乱数に基づいて第１秘密鍵と公開鍵とを生成し、公開鍵を送信して、暗号化された第２秘密鍵を受信する。そして、この第２秘密鍵を第１秘密鍵と公開鍵により復号化して、以降、この復号化した第２秘密鍵によりデータを暗号化して送信する。

【００３１】この通信端末装置では、乱数に基づいて第１秘密鍵と公開鍵を生成することができるので、いちいち操作パネルなどを操作して、これらの鍵のデータを設定する必要がなく、秘密鍵方式の暗号通信に用いる秘密鍵自身の暗号通信の安全性を保つことができる。請求項２では、乱数に基づいて生成された公開鍵を受信すると、この公開鍵により第２秘密鍵を暗号化して返信する。すると、第２秘密鍵で暗号化されたデータを受信するので、このデータを第２秘密鍵により復号化すればよい。したがって、予め第２秘密鍵を設定しておけば、これを定期的に設定し直さなくても、秘密鍵方式の暗号通信の安全性を保つことが出来る。

【００３２】請求項３に記載の暗号通信方法では、送信側は、乱数に基づいて第１秘密鍵と公開鍵とを生成し、一方の受信側は、受信した公開鍵により、秘密鍵方式の暗号通信に使用する秘密鍵自身を暗号化して送信側に返信する。これによって、送信側と受信側のいずれにおいても、意識的に設定データを変更することなく、簡単に安全性が高い暗号通信を実施できるようになる。

【図面の簡単な説明】

【図１】本発明に係る通信端末装置の構成の一例を示したブロック図である。

【図２】本発明に係る暗号通信方法の一例を示した図である。

【図３】本発明に係る通信端末装置のデータ送信時の動

作の一例を示したフローチャートである。

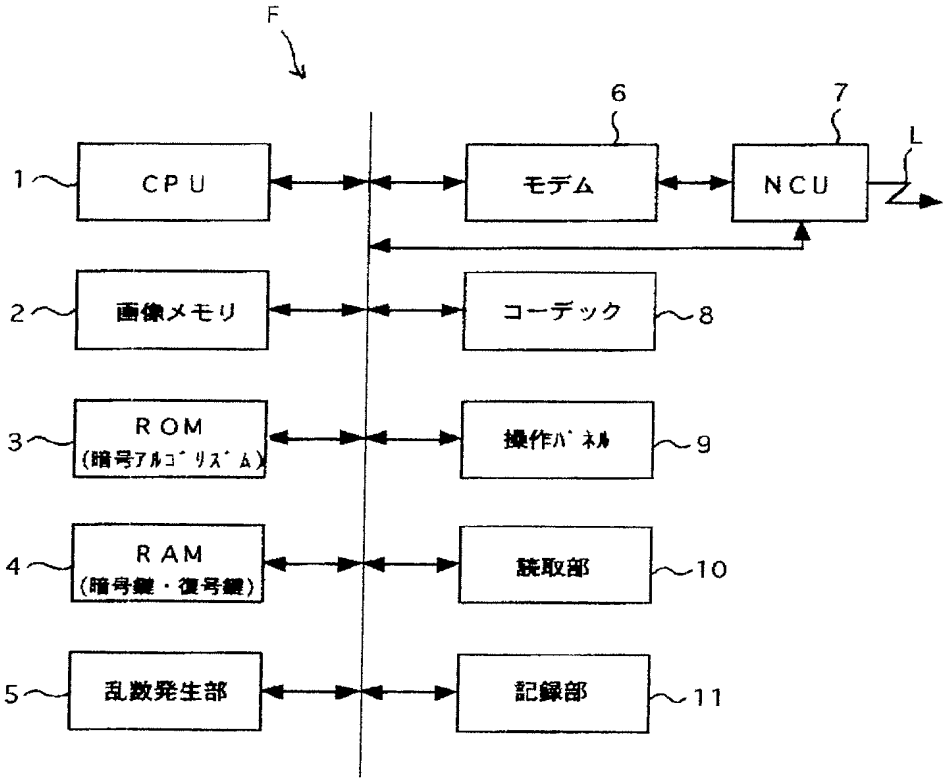
【図４】本発明に係る通信端末装置のデータ受信時の動作の一例を示したフローチャートである。

【符号の説明】

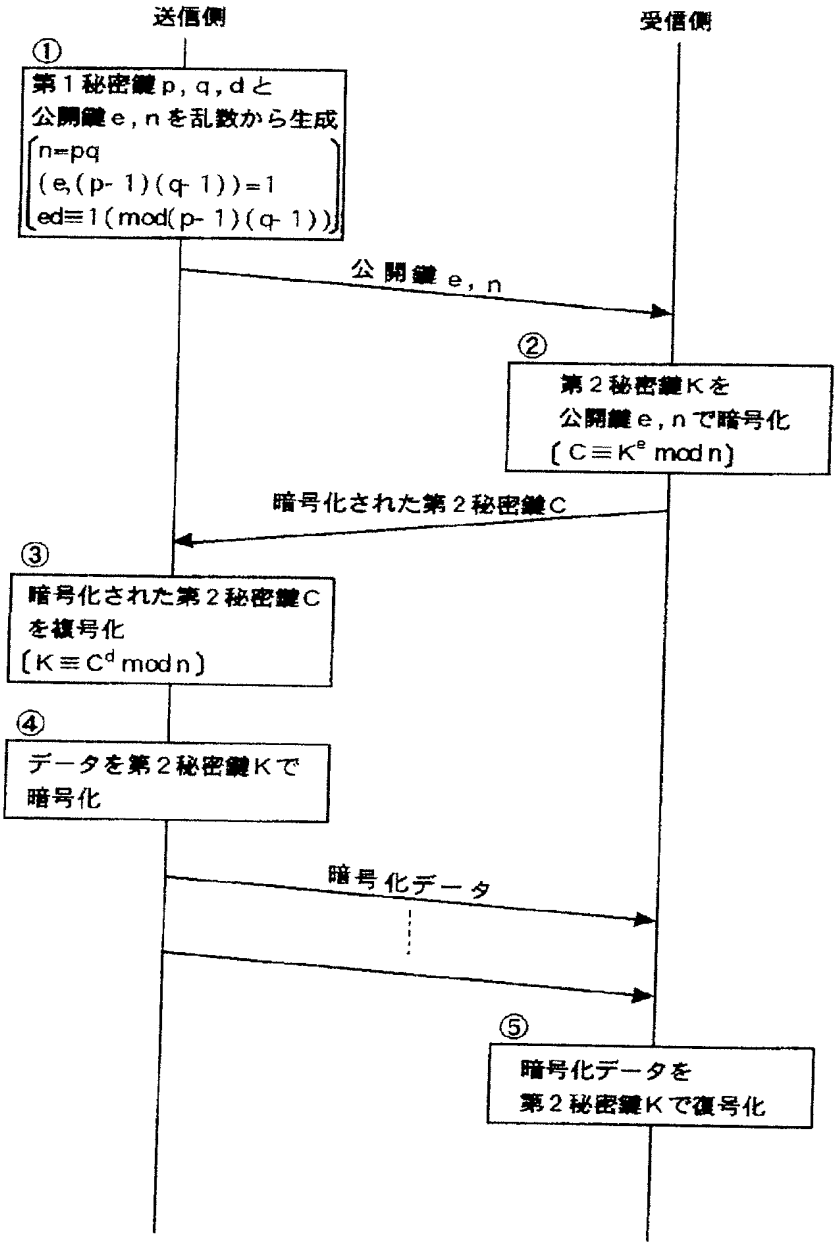
Ｆ・・・ファクシミリ装置　＊

＊１・・・ＣＰＵ
３・・・ＲＯＭ
４・・・ＲＡＭ
５・・・乱数発生部

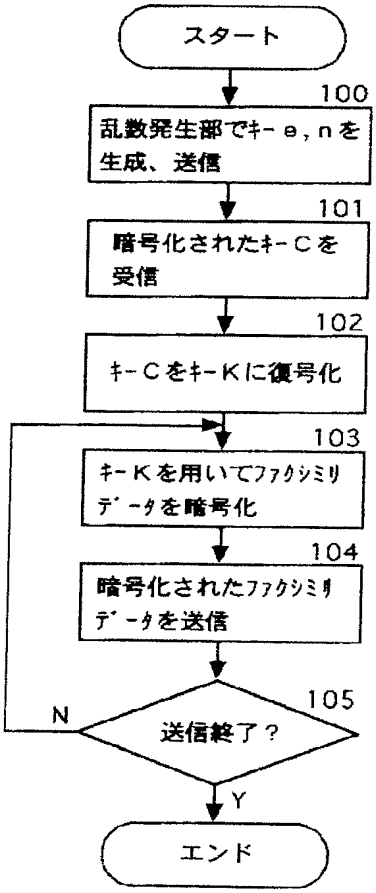
【図１】



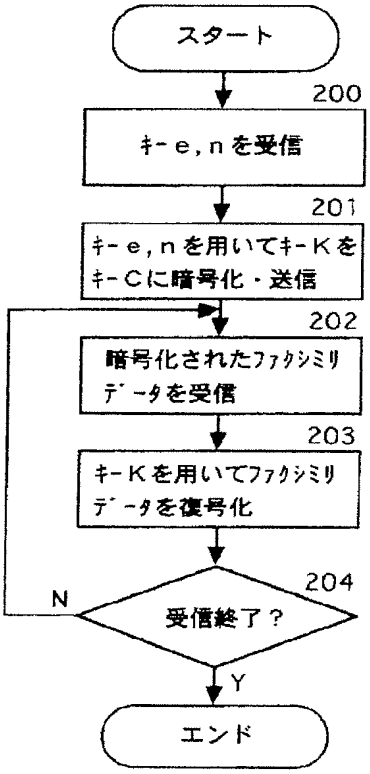
【図２】


送信側
受信側
①
第１秘密鍵ｐ，ｑ，ｄと
公開鍵ｅ，ｎを乱数から生成
n=pq
(e,(p-1)(q-1))=1
ed≡1(mod(p-1)(q-1))
公開鍵ｅ，ｎ
②
第２秘密鍵Ｋを
公開鍵ｅ，ｎで暗号化
〔C≡K^e mod n〕
暗号化された第２秘密鍵Ｃ
③
暗号化された第２秘密鍵Ｃ
を復号化
〔K≡C^d mod n〕
④
データを第２秘密鍵Ｋで
暗号化
暗号化データ
⑤
暗号化データを
第２秘密鍵Ｋで復号化

【図３】


スタート
100
乱数発生部でｷｰ ｅ，ｎを
生成、送信
101
暗号化されたｷｰ Ｃを
受信
102
ｷｰ Ｃをｷｰ Ｋに復号化
103
ｷｰ Ｋを用いてﾌｧｸｼﾐﾘ
ﾃﾞｰﾀを暗号化
104
暗号化されたﾌｧｸｼﾐﾘ
ﾃﾞｰﾀを送信
105
送信終了？
N
Y
エンド

【図４】


スタート
200
ｷｰｅ，ｎを受信
201
ｷｰｅ，ｎを用いてｷｰＫを
ｷｰＣに暗号化・送信
202
暗号化されたﾌｧｸｼﾐﾘ
ﾃﾞｰﾀを受信
203
ｷｰＫを用いてﾌｧｸｼﾐﾘ
ﾃﾞｰﾀを復号化
204
受信終了？
N
Y
エンド